DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY FORCES COMMAND
1777 HARDEE AVENUE SW
FORT MCPHERSON GA 30330-1062

REPLY TO
ATTENTION OF

AFOP-OC

FEB 1 7 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Operations Security (OPSEC) Guidance for Improvised Explosive Devices (IED) Countermeasures - Memorandum # 2

1. Operations Security is a command responsibility. Commanders and agency heads will ensure that their organization's plan implements appropriate OPSEC measures to preserve essential secrecy in every phase of an operation, exercise, test or activity. Department of the Army leadership remains concerned regarding Soldiers sending sensitive information over the internet, including photos of battle damaged military vehicles. It is reasonable to believe that any information released on the internet will be obtained by our adversaries and assist them in identifying vulnerabilities of military equipment, facilities or personnel. This, in turn, allows our adversaries to modify their tactics to more effectively target friendly forces.

2. Improvised Explosive Devices (IED) are the single most significant threat to deployed U.S. forces. They are the primary source of U.S. casualties. Our adversaries actively study our national media, accessible web sites, private, professional and technological forums to gain insight about our tactics, techniques and procedures (TTP) with respect to IED's. Their ability to rapidly exploit our open source information is matched only by their ability to disseminate information on the World Wide Web with near real time speed.

3. It is essential that we protect all IED Countermeasures including: technology solutions, TTP, images of IED damage to vehicles, equipment and organizational/ doctrinal initiatives. For example, briefings that are designed to impart information to Soldiers who are preparing for deployment are not suitable for presentation or release to media.

4. The following information will never be released and only discussed in secure forums:

f. Adversary IED tactics, techniques and procedures (TTP), and analysis of adversary vulnerabilities.

b. Vulnerabilities of friendly force equipment, technologies, organizations or operations.

c. Sensitive photos or images that show battle damage assessment and/or damage linked to specific cause or date/location and fatalities.

d. Specific friendly-force technology areas or details, organizational initiatives and operational TTP designed to counter IEDs.

5. The Army must maintain security to deny the enemy sensitive information. Operational security is essential to prevent the Army's response to IEDs from contributing to adversary objectives and preventing IED-related casualties. Information on IEDs must be disseminated through the use of secure means to ensure it is available to friendly forces only.

6. Media will not be provided images that portray vehicles destroyed by IEDs, in order to protect the information from enemy exploitation. Images of this nature can be used by our adversaries to develop, analyze and/or refine their tactics, techniques and procedures (TTP), thus exploiting U.S. and Coalition efforts in IED Defeat. Interaction with the media, in an official capacity, for information concerning IED Defeat must be routed through PA channels, OPSEC Officer, Operations Officer and Legal Officer.

7. Forces Command deployed forces will continue to respond to the IED threat by employing a multi-response capability that addresses the tenets of IED Defeat, which are:

a. PREDICT actions and circumstances that can affect the ability of the force to maintain momentum.

b. DETECT indicators of impediments or lack of impediments to battlefield mobility early; identify alternatives and establish surveillance.

c. PREVENT potential impediments to battlefield mobility of the force.

d. AVOID detected impediments to battlefield mobility of the force.

e. NEUTRALIZE reduce or overcome (breach) impediments to battlefield mobility that cannot be prevented or avoided.

f. PROTECT Soldiers and vehicles against effects of explosives.

8. Un-secure propagation of sensitive unclassified (FOUO) and classified information, defined in ALARACT message 032/2004 OPSEC NOTICE TO ALL ARMY PERSONNEL, DTG: 091913Z Mar 04, must cease immediately.

9. Chief of Staff of the Army (CSA) and Vice Chief of Staff of the Army (VCSA) OPSEC Guidance memoranda, will be distributed down to company level. Direct all units to utilize the chain teaching model to ensure all Soldiers receive training on the memoranda, power point presentation entitled "OPSEC and the World Wide Web" and the CSA OPSEC video.

10. It is vital that Department of the Army Soldiers, civilians and contractors exercise great caution in discussing information related to work, regardless of their duties. Do not conduct any work-related conversations in common areas, public places, while commuting, or over unsecured electronic circuits. Classified information may be discussed only in authorized spaces, with persons having a specific need to know and the proper security clearance. Unclassified (FOUO) information may likewise require protection because it can often be compiled to reveal sensitive conclusions. Much of the information we use to conduct operations must be withheld from public release because of its sensitivity. If in doubt, do not release or discuss official information.

11. Immediate compliance from all Major Subordinate Commands (MSC) regarding security of IED countermeasures and TTPs associated with them is required. Operations Security must remain Priority One!

12. Contact Ms. Barbara LaChapelle for additional information at DSN 367-5916, COM 404-464-5916, email lachapeb@forscom.army.mil.

FOR THE COMMANDER:

THOMAS G. MILLER
Major General, USA
Deputy Chief of Staff, G-3/5/7

DISTRIBUTION:
COMMANDER
FIRST UNITED STATES ARMY

DISTRIBUTION: (CONT)
THIRD UNITED STATES ARMY
FIFTH UNITED STATES ARMY
UNITED STATES ARMY RESERVE COMMAND
UNITED STATES ARMY SIGNAL COMMAND
I CORPS AND FORT LEWIS
III CORPS AND FORT HOOD
XVIII AIRBORNE CORPS AND FORT BRAGG
1ST CAVALRY DIVISION
3D INFANTRY DIVISION (MECH) AND FORT STEWART
4TH INFANTRY DIVISION (MECH)
7TH INFANTRY DIVISION (LIGHT) AND FORT CARSON
10TH MOUTAIN DIVISION (LIGHT) AND FORT DRUM
24TH INFANTRY DIVISION (MECH) AND FORT RILEY
101ST AIRBORNE DIVISON (AIR ASSAULT) AND FORT CAMPBELL
JOINT READINESS TRAINING CENTER AND FORT POLK
NATIONAL TRAINING CENTER AND FORT IRWIN
III CORPS ARTILLERY
JOINT TASK FORCE SIX
32D AIR DEFENSE ARTILLERY AND MISSILE DEFENSE COMMAND
AIR TRAFFIC SERVICES COMMAND
FORT MCPHERSON
7TH TRANSPORTATION GROUP
20TH SUPPORT COMMAND
52D ORDNANCE GROUP
36TH ENGINNER GROUP